(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－175475

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
13/00	３５１	13/00	３５１Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ
12/54		11/20	１０１Ｂ

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平9－341570

(22)出願日　平成９年(1997)12月11日

特許法第30条第１項適用申請有り　1997年11月６日～11月７日　社団法人情報処理学会開催の「第85回マルチメディア通信と分散処理研究会」において文書をもって発表

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　清水　亮博
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　山中　頭次郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

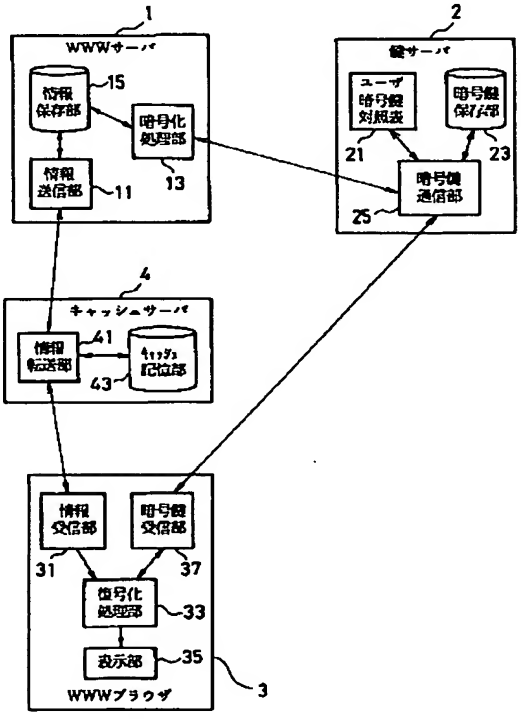
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　アクセス制御方法およびアクセス制御プログラムを記録した記録媒体

(57)【要約】

【課題】　ネットワークキャッシュによる情報提供者であるＷＷＷサーバの負荷およびネットワーク自体の負荷を軽減しつつ条件を満たす利用者のみにコンテンツの閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体を提供する。

【解決手段】　ＷＷＷサーバ１にコンテンツを予め暗号化して記憶し、この暗号化コンテンツをＷＷＷブラウザ３でメッセージとして受信し、該メッセージのトランスファーエンコーディングヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバ２に送信し、鍵サーバ２においてはＷＷＷブラウザ３から受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をＷＷＷブラウザ３に返送し、ＷＷＷブラウザ３は暗号鍵で暗号化コンテンツを復号する。



1

【特許請求の範囲】

【請求項１】　インターネットにおけるＷＷＷサーバとＷＷＷブラウザを有する情報提供システムにおいて、ＷＷＷサーバはコンテンツを予め暗号化して記憶し、ＷＷＷブラウザからの情報要求に対して前記暗号化されたコンテンツをメッセージとしてＷＷＷブラウザに配送し、所定の条件を満たすＷＷＷブラウザにのみ暗号を解く暗号鍵を別途配送し、ＷＷＷブラウザは該暗号鍵で前記暗号化されたコンテンツを復号化することを特徴とするアクセス制御方法。

【請求項２】　前記ＷＷＷブラウザに暗号化鍵を別途配送する処理は、前記暗号化されたコンテンツを含むメッセージを受け取ったＷＷＷブラウザが該メッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバはＷＷＷブラウザから受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をＷＷＷブラウザに返送することを特徴とする請求項１記載のアクセス制御方法。

【請求項３】　インターネットにおけるＷＷＷサーバとＷＷＷブラウザを有する情報提供システムにおいて、ＷＷＷサーバにおいてはコンテンツを予め暗号化して記憶しておき、この暗号化されたコンテンツをＷＷＷブラウザからＷＷＷサーバに要求してメッセージとしてＷＷＷブラウザで受信し、ＷＷＷブラウザはこの受信したメッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバにおいてはＷＷＷブラウザから受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をＷＷＷブラウザに返送し、ＷＷＷブラウザは該暗号鍵で前記暗号化されたコンテンツを復号することを特徴とするアクセス制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットにおいてＷＷＷ (World Wide Web) を使用して情報提供を行う際に有料コンテンツの保護またはセキュリティ保持のために利用者を制限すべく所定の条件を満たす利用者のみに情報の閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】インターネットの発展と、ＷＷＷの普及につれて、様々な情報がインターネット上で提供されるようになっている。同時に情報をある特定の利用者にのみ見せたいとのニーズが高まっている。有料のコンテンツならば利用料を支払ったものだけに、秘密情報ならばそれを見る権限がある者だけに見せたい。ある条件を満たす者にのみ情報の閲覧を許す技術をアクセス制御と呼ぶ。

2

【０００３】従来のアクセス制御は、ＷＷＷサーバの情報転送機能と一体のものとして実現されていた。すなわち、条件を満たす利用者に予めＩＤとパスワードを発行し、ＷＷＷサーバへの情報要求の際に正しいＩＤとパスワードを入力しないと情報の転送自体を行わないとするものである。

【０００４】

【発明が解決しようとする課題】上述した従来のアクセス制御方法は、ネットワークキャッシュ技術との整合性が悪いという問題がある。

【０００５】ネットワークキャッシュ技術は、よく利用されるコンテンツをキャッシュサーバに保存しておき、そのコンテンツの要求に対してはＷＷＷサーバの代わりにキャッシュサーバが情報の転送を行うものであり、ＷＷＷサーバとネットワークの負荷を軽減できるため、近年急速に普及している。

【０００６】しかしながら、キャッシュサーバは、情報要求が条件を満たす利用者からのものであるのかどうか判断できないため、従来型のアクセス制御が行われているコンテンツの代理転送を一切行わないので、ネットワークキャッシュによるＷＷＷサーバおよびネットワークの負荷を軽減することができないというメリットを享受できないという問題がある。

【０００７】本発明は、上記に鑑みてなされたもので、その目的とするところは、ネットワークキャッシュによる情報提供者であるＷＷＷサーバの負荷およびネットワーク自体の負荷を軽減しつつ条件を満たす利用者のみにコンテンツの閲覧を許容するアクセス制御方法およびアクセス制御プログラムを記録した記録媒体を提供することにある。

【０００８】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、インターネットにおけるＷＷＷサーバとＷＷＷブラウザを有する情報提供システムにおいて、ＷＷＷサーバはコンテンツを予め暗号化して記憶し、ＷＷＷブラウザからの情報要求に対して前記暗号化されたコンテンツをメッセージとしてＷＷＷブラウザに配送し、所定の条件を満たすＷＷＷブラウザにのみ暗号を解く暗号鍵を別途配送し、ＷＷＷブラウザは該暗号鍵で前記暗号化されたコンテンツを復号化することを要旨とする。

【０００９】請求項１記載の本発明にあっては、ＷＷＷサーバはコンテンツを予め暗号化して記憶し、ＷＷＷブラウザからの要求に対して暗号化コンテンツをＷＷＷブラウザに配送し、所定の条件を満たすＷＷＷブラウザにのみ暗号を解く暗号鍵を別途配送し、ＷＷＷブラウザは該暗号鍵で暗号化コンテンツを復号化するため、ネット

ワークキャッシュ技術を有効に活用でき、WWWサーバの負荷およびネットワークの負荷を軽減することができる。すなわち、コンテンツを閲覧し得るか否かはWWWサーバでの情報の転送の許可、不許可でなく、WWWブラウザ側の利用者が暗号を解く鍵を持っているか否かであり、コンテンツは暗号化されているため、コンテンツの転送は無条件に許可され、誰にでも可能であり、キャッシュサーバにコンテンツを保持することができ、WWWサーバおよびネットワークの負荷を軽減することができる。

【００１０】また、請求項２記載の本発明は、請求項１記載の発明において、前記WWWブラウザに暗号化鍵を別途配送する処理が、前記暗号化されたコンテンツを含むメッセージを受け取ったWWWブラウザが該メッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバはWWWブラウザから受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をWWWブラウザに返送することを要旨とする。

【００１１】請求項２記載の本発明にあっては、暗号化コンテンツを含むメッセージを受け取ったWWWブラウザはメッセージのトランスファーエンコーディングヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバはWWWブラウザからのユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をWWWブラウザに返送するため、暗号化されたコンテンツを暗号鍵で復号化した場合のみコンテンツを閲覧でき、ネットワークキャッシュ技術を有効活用でき、WWWサーバの負荷およびネットワークの負荷を軽減することができる。なお、トランスファーエンコーディングヘッダはWWWサーバが用意するもので、そこに該当の暗号鍵のＩＤと登録されている鍵サーバのＩＰアドレスが記入されている。

【００１２】更に、請求項３記載の本発明は、インターネットにおけるWWWサーバとWWWブラウザを有する情報提供システムにおいて、WWWサーバにおいてはコンテンツを予め暗号化して記憶しておき、この暗号化されたコンテンツをWWWブラウザからWWWサーバに要求してメッセージとしてWWWブラウザで受信し、WWWブラウザはこの受信したメッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバにおいてはWWWブラウザから受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に前記暗号鍵をWWWブラウザに返送し、WWWブラウザは該暗号鍵で前記暗号化されたコンテンツを復号するアクセス制御プログラムを記録媒体に記録していることを要旨とする。

【００１３】請求項３記載の本発明にあっては、WWWサーバにコンテンツを予め暗号化して記憶しておき、この暗号化コンテンツをWWWブラウザで受信し、トランスファーエンコーディングヘッダから鍵サーバのＩＰアドレスを調べ、暗号鍵ＩＤとユーザ認証情報を鍵サーバに送信し、鍵サーバにおいてはWWWブラウザから受け取ったユーザ情報より暗号鍵ＩＤに該当する暗号鍵のアクセス権が存在しているかどうかを調べ、存在する場合に暗号鍵をWWWブラウザに返送し、WWWブラウザは暗号鍵で暗号化コンテンツを復号するアクセス制御プログラムを記録媒体として記録しているため、該記録媒体を利用して、その流通性を高めることができる。

【００１４】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００１５】図１は、本発明の一実施形態に係るアクセス制御方法を実施するシステム構成を示すブロック図である。図１において、１は情報の記憶および配送を行うWWWサーバ、２は暗号鍵の管理およびアクセス条件のチェックを行う鍵サーバ、３はWWWサーバ１に対して情報を要求し、WWWサーバ１から配送された情報を利用者に表示するWWWブラウザ、４はWWWサーバ１の情報を一時的に蓄積し、WWWサーバ１に代わって情報の配送を行うキャッシュサーバである。

【００１６】WWWサーバ１は、情報送信部１１、暗号化処理部１３および情報保存部１５から構成されている。情報送信部１１は、WWWブラウザ３からの情報要求を受け取り、この要求された情報であるコンテンツを情報保存部１５から取り出し、WWWブラウザ３に配送する。この時、コンテンツを暗号化して配送する場合には、配送メッセージのトランスファーエンコーディング(Transfer-Encoding) ヘッダによって暗号化されていることを示す。暗号化処理部１３は、本アクセス制御方法のためのコンテンツの暗号化と鍵の鍵サーバ２への登録を行う。情報保存部１５は、コンテンツおよび本アクセス制御方法の管理情報を記憶する。

【００１７】鍵サーバ２は、ユーザ暗号鍵対照表２１、暗号鍵保存部２３および暗号鍵通信部２５から構成されている。ユーザ暗号鍵対照表２１は、利用者と該利用者がアクセス権を有する暗号鍵を対応して表形式に記憶する。暗号鍵保存部２３は、WWWサーバ１から渡された暗号鍵を保存する。暗号鍵通信部２５は、WWWサーバ１から暗号鍵およびアクセス情報を受け取って、ユーザ暗号鍵対照表２１および暗号鍵保存部２３に保存する。また、暗号鍵通信部２５は、WWWブラウザ３から暗号鍵の要求を受け取り、この要求してきた利用者のアクセス権の有無をユーザ暗号鍵対照表２１から調べ、アクセス権があれば暗号鍵をWWWブラウザ３に送る。

5

【００１８】WWWブラウザ３は、情報受信部３１、復号化処理部３３、表示部３５および暗号鍵受信部３７から構成されている。情報受信部３１は、WWWサーバ１に情報要求を送り、その応答を受信する。復号化処理部３３は、情報受信部３１を介してWWWサーバ１から受信した応答が暗号化されている場合に復号化を行う。表示部３５は、復号化処理部３３からの応答を表示する。暗号鍵受信部３７は、鍵サーバ２に対して暗号鍵の要求を行い、鍵サーバ２から暗号鍵を受け取り、復号化処理部３３に供給する。

【００１９】キャッシュサーバ４は、情報転送部４１およびキャッシュ記憶部４３から構成されている。情報転送部４１は、WWWブラウザ３からの情報要求をWWWサーバ１に中継し、WWWサーバ１からの応答をWWWブラウザ３に送るとともに、この応答をキャッシュ記憶部４３に記憶しておく。なお、キャッシュサーバ４は通常のWWWで使用されるものと同一であり、本発明に固有な機能を特に必要としない。

【００２０】次に、図２～図５を参照して、図１に示す実施形態の作用を説明する。

【００２１】図２は、WWWサーバ１がWWWブラウザ３と通信する場合の通信制御処理を示すフローチャートである。図２において、WWWサーバ１は、WWWブラウザ３からの要求を受け付けると（ステップＳ１１）、該要求を解釈して応答メッセージを用意する（ステップＳ１３）。この時、WWWサーバ１は、WWWブラウザ３から要求された情報が暗号化されている場合には、（１）応答メッセージ本体が暗号化されていることを示す識別子、（２）鍵サーバ２のＩＰアドレスを示す識別子、（３）要求された情報を暗号化した暗号鍵の識別子を応答メッセージのトランスファーエンコーディング・ヘッダに添付して、WWWブラウザ３に返送する（ステップＳ１７，Ｓ１９）。

【００２２】次に、図３に示すフローチャートを参照して、WWWブラウザ３がWWWサーバ１から応答メッセージを受け取って表示するまでの処理について説明する。

【００２３】図３において、WWWブラウザ３は、WWWサーバ１から応答メッセージを受信すると（ステップＳ２１）、メッセージのトランスファーエンコーディング・ヘッダに「メッセージ本体が暗号化されている」ことを示す識別子があるか否かをチェックする（ステップＳ２３）。該識別子がある場合には、前記トランスファーエンコーディング・ヘッダから鍵サーバ２のＩＰアドレスと暗号鍵のＩＤを取得する（ステップＳ２５）。それから、この取得したＩＰアドレスが示す鍵サーバ２と通信を行って、該鍵サーバ２からＩＤに該当する暗号鍵を受け取る（ステップＳ２７）。そして、この暗号鍵を使用して、WWWサーバ１から受け取ったメッセージを復号化し（ステップＳ２９）、この復号化したメッセージを表示部３５に表示する（ステップＳ３１）。

6

【００２４】次に、図４に示すフローチャートを参照して、鍵サーバ２とWWWブラウザ３との間における暗号鍵の受渡し処理について説明する。なお、図４において左側に示すフローチャートはWWWブラウザ３の暗号鍵受信処理を示し、右側のフローチャートは鍵サーバ２の鍵送信処理を示している。

【００２５】図４において、鍵サーバ２がWWWブラウザ３からの接続を待っている状態において（ステップＳ５１）、WWWブラウザ３が鍵サーバ２に接続されると（ステップＳ４１）、鍵サーバ２はサーバ認証情報をWWWブラウザ３に送信する（ステップＳ５２）。WWWブラウザ３は鍵サーバ２からサーバ認証情報を受信すると（ステップＳ４２）、該サーバ認証情報を検査し、正しいサーバであることを確認する（ステップＳ４３）。

【００２６】WWWブラウザ３は、サーバ認証情報の確認後、ユーザ認証情報を鍵サーバ２に送信する（ステップＳ４４）。鍵サーバ２は、WWWブラウザ３からのユーザ認証情報を受信すると（ステップＳ５３）、この受信したユーザ認証情報を検査し、正しいユーザであるか否かを検査する（ステップＳ５４）。WWWブラウザ３は、続いて暗号鍵の識別子を鍵サーバ２に送信する（ステップＳ４５）。鍵サーバ２は、前記ユーザ認証情報から正しいユーザであることを確認し、更にWWWブラウザ３から暗号鍵の識別子を受信すると（ステップＳ５５）、鍵サーバ２は、この受信した暗号鍵の識別子に該当する暗号鍵に対するアクセス権をユーザが持っているか否かをチェックする（ステップＳ５６）。ユーザが該アクセス権を持っている場合には、鍵サーバ２は暗号鍵をWWWブラウザ３に返送し（ステップＳ５７）、WWWブラウザ３は該暗号鍵を受信する（ステップＳ４６）。

【００２７】次に、図５に示すシーケンス図を参照して、図１に示す実施形態の全体的作用について説明する。図５において、まず情報がキャッシュされていない場合には、WWWブラウザ３からの情報要求はキャッシュサーバ４を経由してWWWサーバ１に送られ、WWWサーバ１は要求された情報を返信する。この返信情報はキャッシュサーバ４に一時的に保存されるとともにキャッシュサーバ４を経由してWWWブラウザ３に送信される。この情報が暗号化されている場合には、WWWブラウザ３は鍵サーバ２に対して暗号鍵を要求する。鍵サーバ２はこの要求に対して暗号鍵をWWWブラウザ３に返送し、WWWブラウザ３はこの暗号鍵を使用して、暗号化情報を復号する。

【００２８】一方、情報がキャッシュされている場合には、WWWブラウザ３からの情報要求は、キャッシュサーバ４にて処理され、キャッシュサーバ４から情報がWWWブラウザ３に返信される。この情報が暗号化されている場合には、同様にWWWブラウザ３は鍵サーバ２に

対して暗号鍵を要求し、鍵サーバ２は暗号鍵をWWWブラウザ３に返送し、WWWブラウザ３はこの暗号鍵を使用して、暗号化情報を復号する。

【００２９】

【発明の効果】以上説明したように、本発明によれば、WWWサーバはコンテンツを予め暗号化して記憶し、WWWブラウザからの要求に対して暗号化コンテンツをWWWブラウザに配送し、所定の条件を満たすWWWブラウザにのみ暗号を解く暗号鍵を別途配送し、WWWブラウザは該暗号鍵で暗号化コンテンツを復号化するので、ネットワークキャッシュ技術を有効に活用でき、WWWサーバの能力が低くても大量の情報配信を行うことができ、多くの利用者に対する有料コンテンツの提供や秘密情報の提供を安価なハードウェアで実現できる。また、ネットワークへの負荷も軽減できるため、大量の情報の配信に伴うネットワークコストの上昇を抑制できる。更に、従来のアクセス制御では、通信の盗難によりコンテンツが漏洩する危険があったが、本発明ではコンテンツは暗号化されているため、このような危険を回避することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るアクセス制御方法を実施するシステム構成を示すブロック図である。

【図２】図１の実施形態においてWWWサーバがWWWブラウザと通信する場合の通信制御処理を示すフローチャートである。

【図３】図１の実施形態においてWWWブラウザがWWWサーバから応答メッセージを受け取って表示するまでの処理を示すフローチャートである。

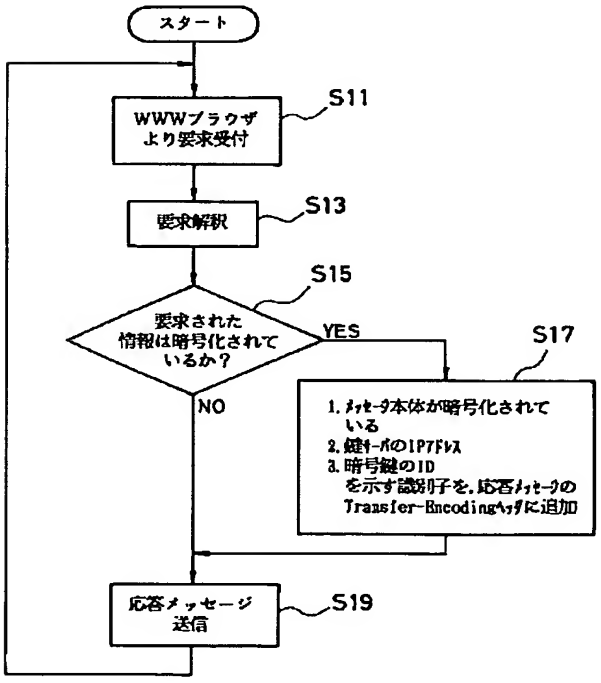
【図４】鍵サーバとWWWブラウザとの間における暗号鍵の受渡し処理を示すフローチャートである。

【図５】図１に示す実施形態の全体的作用を示すシーケンス図である。

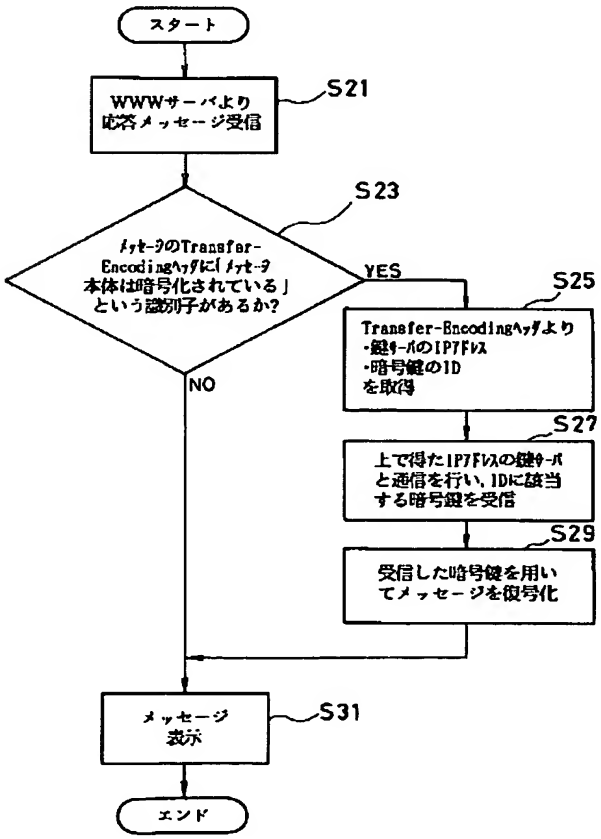
【符号の説明】

１　WWWサーバ
２　鍵サーバ
３　WWWブラウザ
４　キャッシュサーバ
１３　暗号化処理部
１５　情報保存部
２１　ユーザ暗号鍵対照表
２３　暗号鍵保存部
２５　暗号鍵通信部
３３　復号化処理部
３７　暗号鍵受信部
４３　キャッシュ記憶部

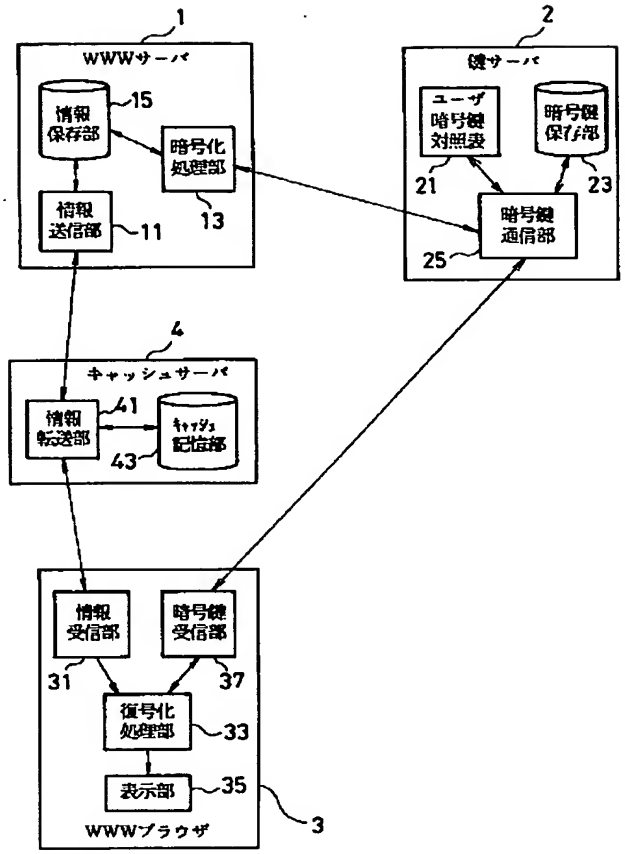
【図２】



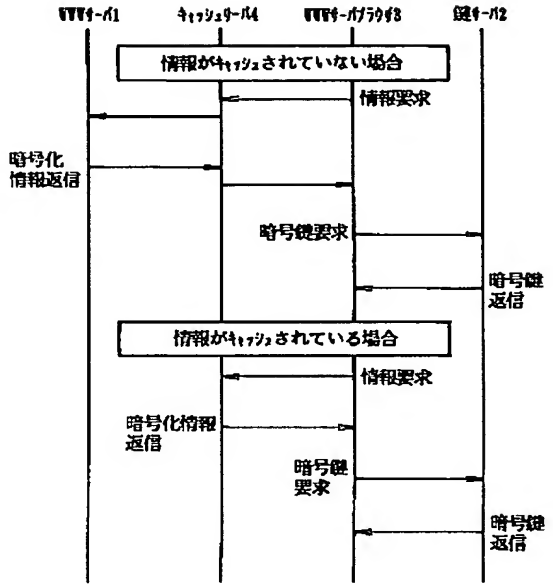
【図３】



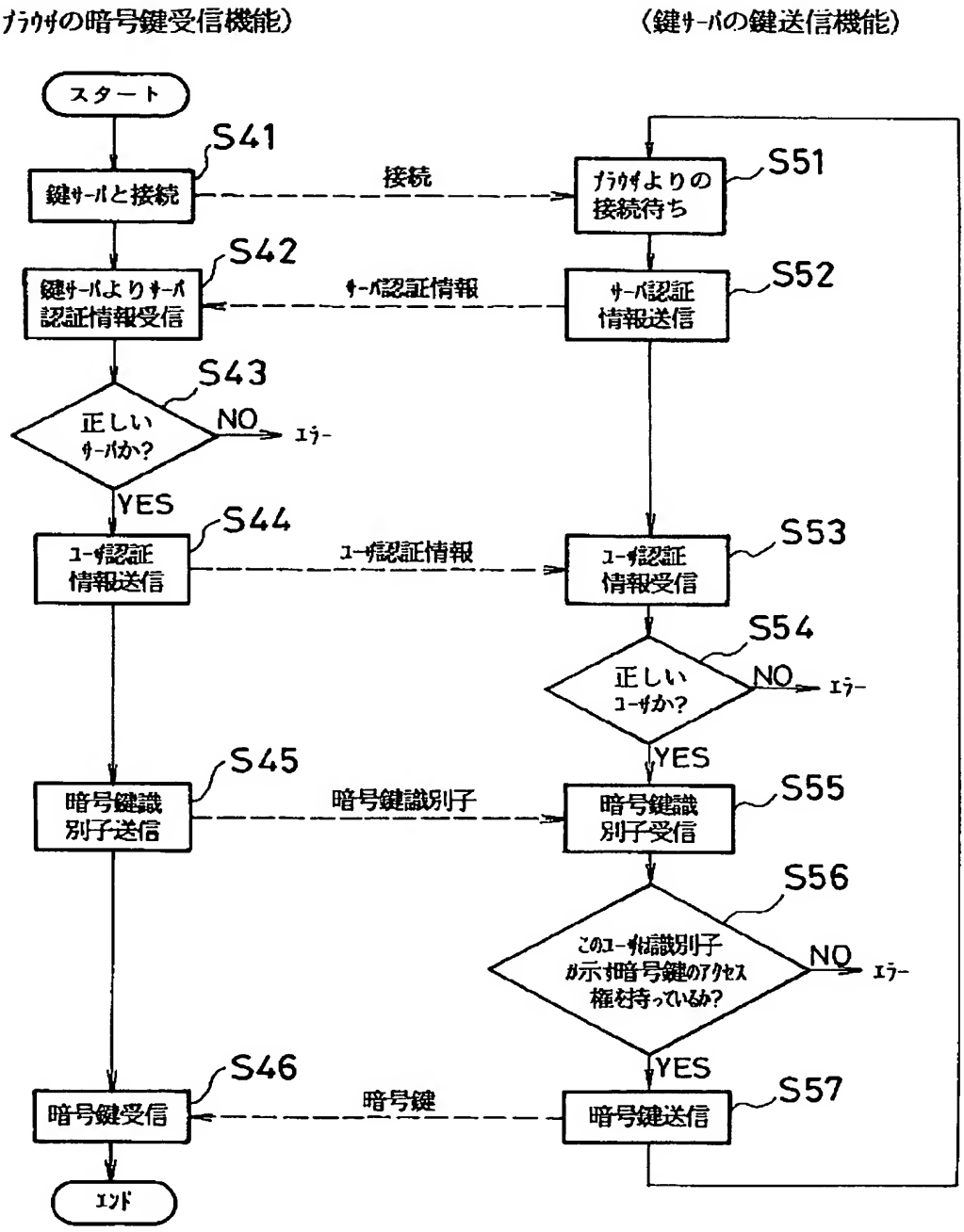
【図１】


1
WWWサーバ
情報保存部
15
暗号化処理部
13
情報送信部
11
2
鍵サーバ
ユーザ暗号鍵対照表
21
暗号鍵保存部
23
暗号鍵通信部
25
4
キャッシュサーバ
情報転送部
41
キャッシュ記憶部
43
情報受信部
31
暗号鍵受信部
37
復号化処理部
33
表示部
35
WWWブラウザ
3

【図５】


WWWサーバ1
キャッシュサーバ4
WWWブラウザ3
鍵サーバ2
情報がキャッシュされていない場合
情報要求
暗号化情報返信
暗号鍵要求
暗号鍵返信
情報がキャッシュされている場合
情報要求
暗号化情報返信
暗号鍵要求
暗号鍵返信

【図４】



フロントページの続き

(51) Int. Cl.[6]　　識別記号　　F I

H０４L　12/58